Agency Centralized IT Reference Model ©

For State of Minnesota Agencies' Planning and Management

Version 2.0

March 8, 2012

658 Cedar Street Saint Paul, MN 55155 www.oet.state.mn.us

PROVIDING THE LEADERSHIP AND SERVICES THAT IMPROVE GOVERNMENT THROUGH THE EFFECTIVE USE OF INFORMATION TECHNOLOGY.

Background

Purpose of the Document

The 2011 State Legislature passed a law requiring the consolidation of state IT staff from 70+ agencies to the Office of Enterprise Technology, under the direction of the State CIO. In order to meet the timeframes in legislation, the first stage of consolidation employed a federated model in which agency CIOs have delegated authority from the State CIO to manage all IT budgets and activity within the agency. Within this model, agency CIOs are required to develop a plan to centralize all IT staff and functions in a common manner in order to facilitate shared services and further consolidation at the enterprise level.

This IT Reference Model has been developed by state agency chief information officers as a reference document for the management of IT resources at individual state agencies. The purpose of the document is to create a common vocabulary and structure that each individual executive branch agency will use as it centralizes IT functions within the agency.

The reference model describes an “end state” by which executive branch IT can be effectively managed at the enterprise and the agency level, and by which IT can best meet the needs of its agency customers.

All agencies will use this reference model as the foundation for internal agency analysis, planning, and process improvement.

The reference model will also serve as a tool at the enterprise level to develop template service level agreements for all IT services, develop a common financial structure for State IT service delivery and accounting, and create a framework for service delivery strategies and the identification of utility and centralized services and functions.

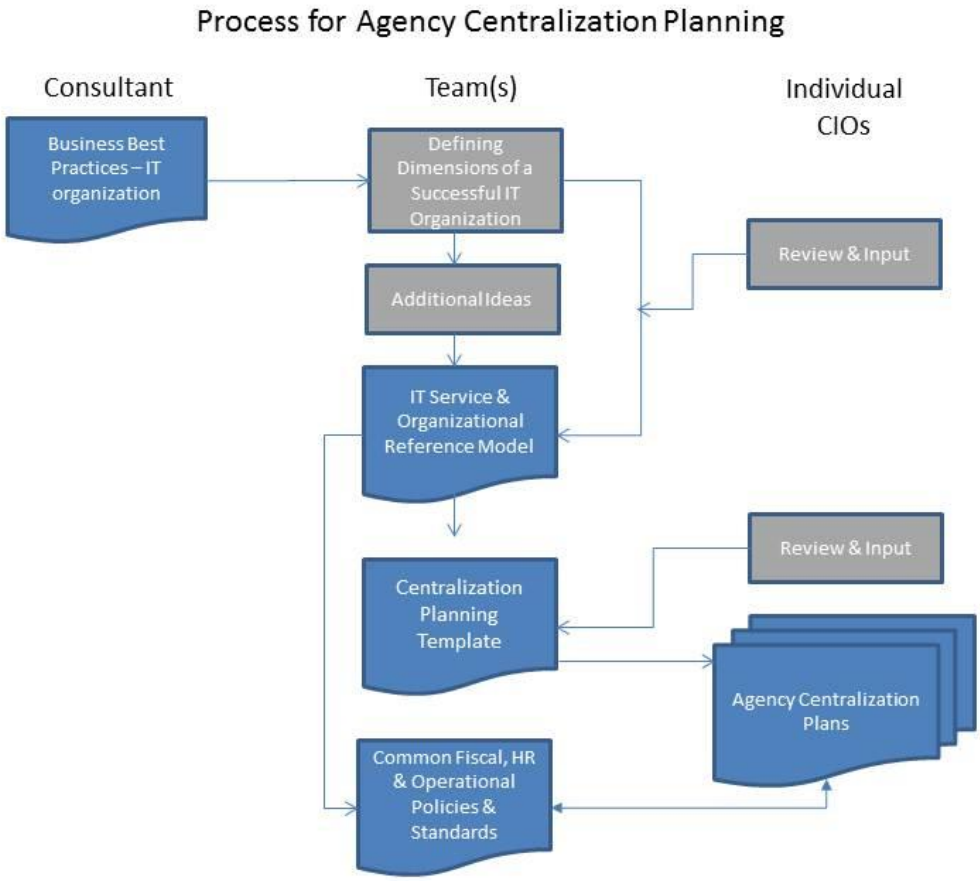
Planning Objectives

The Agency Centralized IT Reference Model is the primary reference document in the individual planning being undertaken by agency CIOs to centralize IT at the agency level. Their planning objectives include:

1. Define the essential organizational attributes that should be common across agencies, including services, functions, processes, and enabling technologies.
2. Ensure that agency IT organizations have a consistent and full-featured suite of services.
3. Develop a threshold of organizational consistency that will allow for enterprise deployments of common procedures and toolsets.
4. Develop a coherent vision for organizing service delivery that can be understood and supported by agency executive customers.
5. Identify agency-specific gaps in capabilities that require management attention and support.
6. Identify opportunities for expertise and resource sharing between agencies.
7. Develop a basis for understanding service delivery costs across the enterprise.
8. Develop a structural and semantic basis for financial management and cost coding guidelines.
9. Identify opportunities for shared service that result in cost efficiencies and improved service.

Planning Process

The development of this model has been done under the aegis of the Agency Centralization Working Team, a team of agency CIOs and OET staff within the IT Consolidation Program. Input has been provided by the agency CIOs and the State CIO.



Planning Process Steps and Deliverables

Business Best Practices: Deliverable from a third party engagement to define industry best practices/models for IT organizations of the size and scope of State of Minnesota state agencies. The deliverable was used by the Agency IT Centralization Working Team and the Agency CIOs to develop a common organizational/functional model for all agencies (included in this document).

Dimensions of a Successful IT Organization: Definition of a successful IT organization, included in this Agency Centralized IT Reference Model.

Agency Centralized IT Reference Model (this document): Reference document to be used by individual agencies in planning and describing the services and organization of IT within a centralized model. Developed by the Agency IT Centralization Working Team and vetted by the agency CIOs.

Centralization Planning Template: Planning template for agencies to use in documenting their plans for centralizing IT at the agency level. The planning template will use this document as its primary reference material.

Agency Centralization Plans: Individual agency plans for centralizing IT within the agency, based on the Centralization Planning Template. Plans will include self-assessment, inventorying, analysis, a description of the "to be" state, and a roadmap for individual agency centralization of services and functions.

Common Fiscal, HR and Operational Policies and Standards: Policies and standards for the operation of IT at the agency and central levels will be developed by several consolidation working teams (HR, Finance, Governance). These policies and standards will be collected and posted to be used by agencies to operate their centralized IT organizations in a common manner.

Term Definitions

For the purposes of this document, the following terms are defined below:

Federated: United under a central organization (OET) with authorization for general operations delegated to satellite (agency) sub-organizations.

State IT organization: The combined organizational construct of the current central organization (OET) and the federated agency IT organizations that are under OET's authority.

Agency centralized organization: The organizational construct at each executive branch agency/entity in which all people and functions defined to be in scope of State IT consolidation are under a single management structure under the delegated authority of the agency CIO.

Enterprise: A combined view of the executive branch IT organization's strategy, management and activity.

Centralized / shared services: Those services that are delivered at a single, enterprise level either by the central IT organization or by an agency center of excellence.

Central IT: The current OET organization that provides direction, policy, and delivers a catalog of shared services under the leadership of the State CIO.

How to Get More Information

This reference model is the first step in a long and iterative process to define the roles, responsibilities and common operating procedures for a complex and changing enterprise IT environment. Inevitably, the first draft of this document will not answer all of the questions that agency staff encounters as they begin planning centralization at the agency level and consolidation at the enterprise level.

Clarifying questions and suggestions for improvement can be posted anytime on the CIO working site (CIOs only have access), and some in-person discussion forums will be scheduled once planning begins.

As necessary, the document will be revised and republished for agency planning purposes.

Dimensions of a Successful IT Organization

The State of Minnesota CIO community has defined the following dimensions of a successful IT organization. These will be the foundation of planning for a common state IT environment, and for planning the IT organization at the agency level.

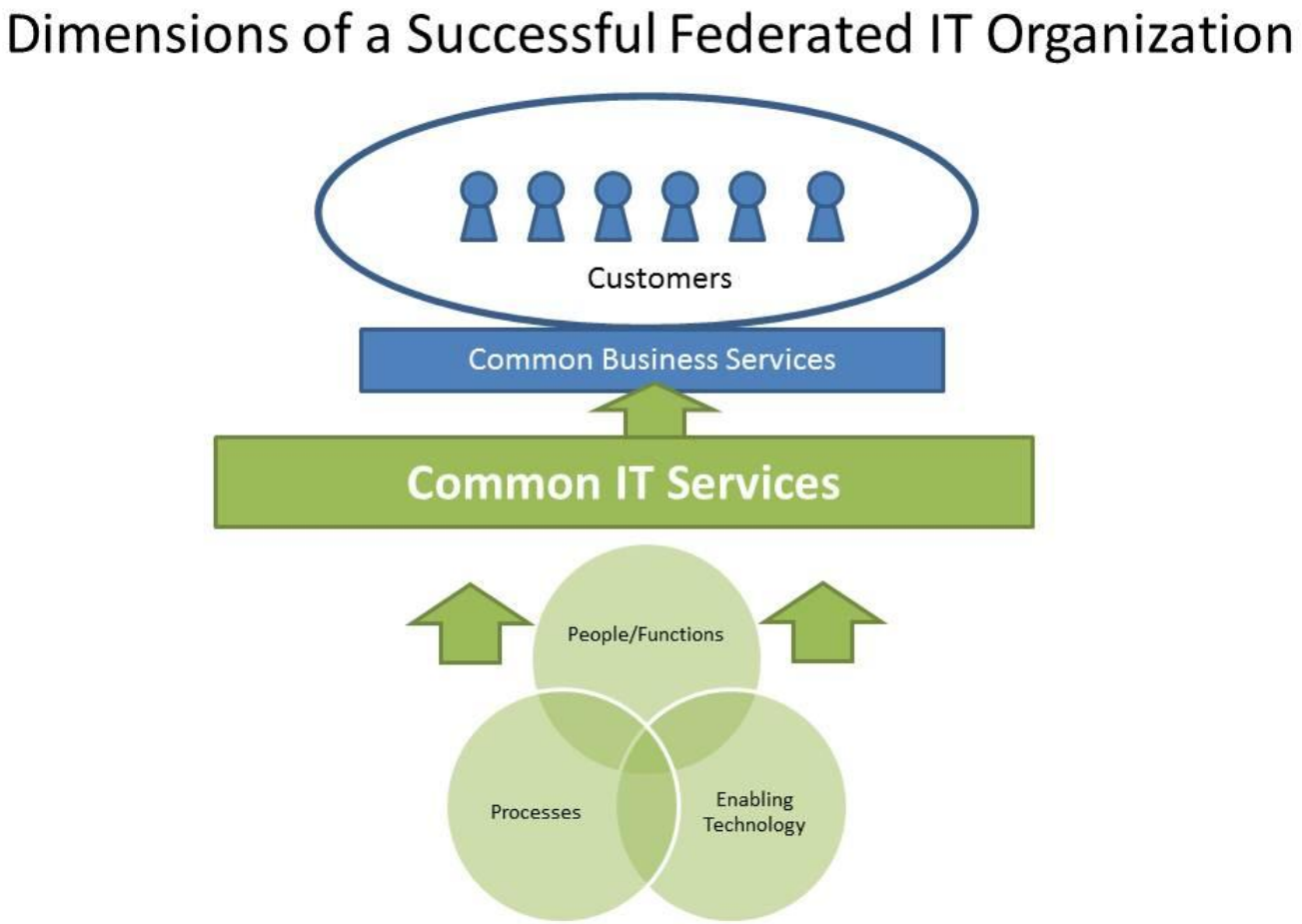
Definitions

Service: A means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific cost and risks. The IT services dimension includes two views: IT services from an IT perspective ("Common IT Services"), which aligns the services with their related IT functions; and IT services from a business perspective ("Common Business Services"), which bundles IT services into consumable groupings that relate to the end-users' business processes and are understandable in business terms.

Process: A structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs and includes any of the roles, responsibilities, tools and management controls required to reliably deliver the outputs.

People/Function: A team or group of people and the tools they use to carry out one or more process or activity.

Enabling Technology: Common technologies used to deliver services and/or manage functions.



Dimension 1: The Services

The goal of this IT Service Reference Model is to develop common definitions and a common service framework for every agency in order to enable cross-collaboration, shared services, and common and comparable service expectations and metrics.

This reference model is intended for the use of agency CIOs and is therefore focused on the common definitions of IT service delivery within an IT organization. It does not attempt to address the business definition of IT services which will be covered in separate documents as the agencies develop common service level agreements for their customers.

State of Minnesota Common IT Services

1. **Infrastructure Services:** All hardware, software, networks, facilities, etc. that are required to develop, test, deliver, monitor, control or support IT Services.
    a. **End User Services** – Services provided directly to end users designed to enable and support computing needs
        i. Workstation management
            1. Enterprise tool provisioning (remote access, etc.)
            2. Office automation (Office, PDF, etc.)
            3. End point defense – Applications and tools responsible for protecting information on computers that routinely interact with untrusted devices on the internet or may be prone to loss or theft
            4. File, Print
        ii. Electronic Collaboration and Communications tools
            1. email, instant messaging (IM),document management (SharePoint), fax
        iii. Voice Communications
            1. Voice support, traditional phone services
            2. Telecommunications infrastructure [voice over internet protocol (VOIP), video]
            3. Field office facility support
        iv. Mobile Device Support
            1. Connectivity and Mobility
            2. Cell phones, global positioning systems (GPS), personal digital assistant (PDA), pagers
        v. Facility Services
            1. Audio/Visual equipment support
            2. Lab and Training room support
    b. **Hosting Services** – Services provided to support platforms required to host applications
        i. Server Support
            1. Installation, operation and maintenance
        ii. Storage and Backup Support
            1. Installation, operation and maintenance
            2. Restores
        iii. Facility Services
            1. Datacenter
        iv. DB and Middleware Operational Support
            1. Maintenance and repair
    c. **Connectivity/Network Services** – Services provided to support end-to-end connectivity and network access

i. Network infrastructure (wide area network (WAN)/local area network (LAN); wireless)
    1. Telecommunications infrastructure (voice over internet protocol (VOIP), video)
ii. Boundary defense, remote access and load management – Applications and tools responsible for separating and controlling access to different networks with different threat levels and sets of users to reduce the number of successful attacks [Source: IT service taxonomy]
iii. Directory services
    1. Active directory, enterprise active directory, domain name services
iv. Facility services
    1. Video conferencing

2. **Application Services:** All aspects of development, management, and support for applications listed in the IT portfolio.
    a. **Application development** – Activities conducted to elicit business requirements, design, build or purchase, and secure information systems.
        i. Business and process analysis
        ii. System research and selection
        iii. System design
        iv. System build
        v. System testing
    b. **Application management** – Activities conducted which encompass a set of best practices proposed to improve the overall quality of IT software development and support through the life-cycle of software development projects.
        i. Application deployment
        ii. Business application operations and support--custom and commercial off-the-shelf (COTS)
        iii. Access management
    c. **Database administration** - Activities conducted and provided that are responsible for the design, implementation, maintenance and repair of an organization's database.
    d. **Middleware administration** – Activities that are responsible for the design, implementation, maintenance and repair of an organization's computer software that connects software components and their applications.
    e. **Data management** – Activities conducted to enable business users to consume and manage data.
        i. Records management
        ii. Information management
        iii. Reporting and decision support
        iv. Business intelligence
    f. **Web design, administration and content coordination** – Activities conducted that manage web server, web design and mechanism to manage content.

3. **Security Services**: Overall management/administration of internal security, risk, and governance for all IT infrastructure and applications.
    a. **Security governance, risk and compliance** – Activities conducted that manage the planning, oversight, coordination, risk management of all information security activities and compliance to established guidelines, specifications or legislation.
        i. **Program Management** – Processes and reporting responsible for the planning, oversight and coordination of all information security activities
        ii. **Training and Awareness** – Programs and events responsible for providing employees at all levels with relevant security information to lessen the number of security incidents

iii. **Compliance** – Activities responsible for either a state of being in accordance with established guidelines, specifications, or legislation or in the process of becoming so.

b. **Information Security Monitoring** – Systems, tools or processes responsible for gaining situational awareness through continuous monitoring of networks and other IT assets for signs of attack, anomalies, and inappropriate activities.
c. **Information Security Incident Response and Forensics** – Systems, tools or processes responsible for determining the cause, scope and impact of incidents to stop unwanted activity, limit damage and prevent recurrence.
d. **Vulnerability and Threat Management** – Systems, tools or processes responsible for continuously identifying and remediating vulnerabilities before they can be exploited.
e. **Identity and Access Management** – Systems, tools or processes responsible for managing the identities of users and devices and controlling access to resources and data based on a need to know.
f. **Facility Services** – Systems, tools or processes responsible for protecting information systems and data from physical threats.
    i. Physical Security

4. **Service Desk**: The single point of contact between the service provider and the users. A typical service desk manages incidents, problems and service requests and also handles communication with the users.

    a. **Technical assistance and end user support** – Systems, tools or processes used to restore and maintain normal service operation as quickly as possible and minimize the adverse effect on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.
        i. Track, log and resolve inquiries
        ii. Service request processing
            1. e.g., Access management
    b. **End-user technical training** – Organized activity aimed at imparting information and/or instructions to improve the recipient's performance or to help him or her attain a required level of knowledge or skill.
    c. **Performance monitoring and reporting** - The assessment and monitoring of the performance of an organization's computer software applications. The goal of application performance management is to diagnose and fix problems within the various software applications in order to reduce errors and inefficiencies.

5. **Leadership**: Overall management to ensure service alignment, provisioning, and conformance to common definitions and principles; advance business improvement; and drive to increased efficiencies.

    a. **IT management** –The maintenance and advancement of IT operations in alignment with enterprise and business objectives, within the constraints of available resources.
        i. Technology assessment and planning
        ii. Enterprise architecture
        iii. Policy, standards, guidelines and procedures
    b. **Strategic planning** – Planning to ensure alignment of enterprise and business vision, values, and strategies for accomplishing an organization's mission.
    c. **Portfolio, program and project management** –The alignment of customer and IT business opportunities with common approaches to cataloging, characterizing, and executing the work.
    d. **Financial and staff management** –The classification and characterization of human resources and financial transactions in a manner consistent with enterprise objectives.
    e. **Governance and customer relationship management** –Maintenance of an on-going capability for validating IT management action through engagement with agency leadership.

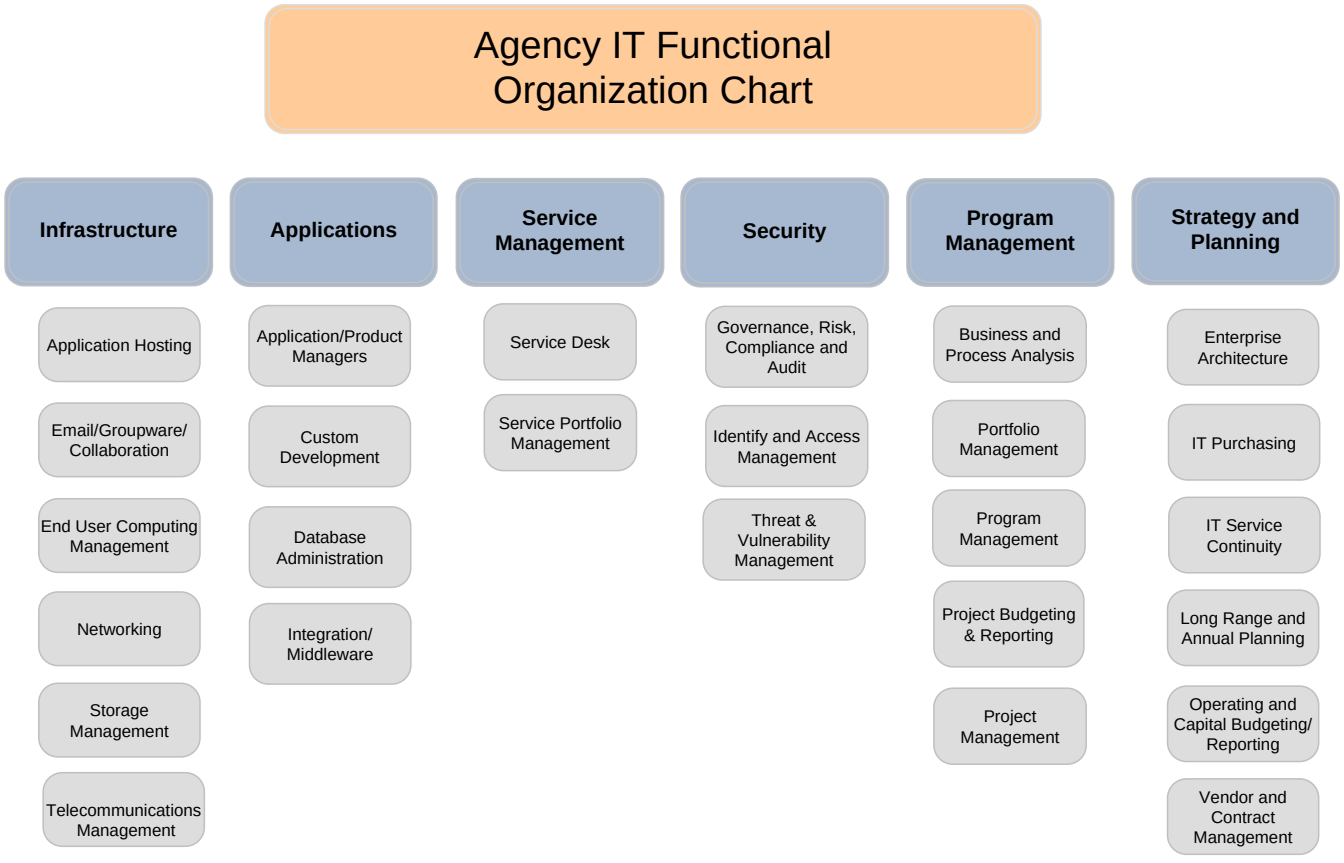
f. **Hardware and software procurement, deployment and decommissioning** – Comprehensive management of hardware and software assets, emphasizing standards and strategic sourcing.
    i. License and contract administration
    ii. Asset Management
g. **IT Service Continuity** – Ensuring that critical business functions will be available in times of crisis.

Dimension 2: The People

The IT Functional Reference Model below represents the "end state" organization that all agencies will develop in order to maximize efficiency, accountability and interoperability in delivering the services defined above. The end state organizational model is structured according to "functions".

By having a common definition of what people do, agencies can create service level agreements that meet business requirements, manage resources to meet service level agreements, account for service expenditures within a common structure, and define common processes and process ownership. A common functional organization structure increases accountability and interoperability at the enterprise level.

Although the functional organization chart resembles the Service Reference Model in its major groupings, it does not mirror the services exactly because it describes "how" we organize to do the work, not "what" services we deliver, focusing on the logical groupings of the people that do the work.



Functional Definitions, Agency IT Organizations

Infrastructure

Application Hosting: Administration of hardware, virtual server processes, and externally hosted resources to support a full range of business and system-support databases and applications. Formerly "Servers," but with expanded definition to include administration of cloud-based resources.

Email/groupware/collaboration: Administration of collaboration deployments in conformance with state and agency standards. Includes non-SharePoint collaboration toolsets.

End User Computing Management (I): Administration of user devices that consume state-hosted network services; including configuration, installation, inventory, and other administrative processes. Formerly workstations, but expanded to include all classes of personal computers.

Networking: Administration of all devices that constitute the full wired and wireless network infrastructure for an agency. Includes application of security policies and network system monitoring.

Storage Management: Administration of shared storage solutions across all application areas (business applications, collaboration, data warehousing). Includes administration of cloud-based resources.

Telecommunications Management: Administration of wired phone and video services, including user administration and scheduling. Includes IP telephony, and where applicable, analog voice systems.

Applications

Application and Product Management: The objective of Application and Product management is to support all applications that reside in the application portfolio and to improve the overall quality of developed or purchased applications.

Custom Development: Custom Development is the development of software specially for a specific organization. As such, it can be contrasted with the use of software packages developed for the mass market, such as commercial off-the-shelf (COTS) software, or existing free software.

Database Administration: The primary purpose of Database Administration is to conduct activities that are responsible for the design, implementation, maintenance and repair of an organization's database(s).

Integration and Middleware: The purpose of the Integration and Middleware function is to perform activities that are responsible for the design, implementation, maintenance and repair of an organization's computer software that connects software components and their applications. In addition, this function provides foundational, common building blocks to applications such as document management and reporting and BI solutions.

Service Management

Service Desk: The primary purposes of a Service Desk include: incident and problem management and the life-cycle management of all service requests. In addition to communicating with customers to keep them informed of progress and advising them on workarounds.

Service Portfolio Management: The objective of Service Portfolio Management is to ensure that the service provider has the right mix of services to meet required business outcomes at an appropriate level of investment. Also included is Service Level Management which monitors service offerings and reports on service metrics.

Security

Governance, Risk, Compliance and Audit: High level business-collaborative planning and analysis resulting in strategies that balance risk and cost, while conforming to established security standards. Governed by industry best practices and legislative expectations.

Identity and Access Management: Development, implementation, and maintenance of a comprehensive approach to centralized customer data store management and access controls. Applicable within a broad domain of contexts, including business application, file shares, and enterprise application access.

Threat and Vulnerability Management: Proactive assessment of hardware and software system components to identify those at elevated risk of attack from malicious forces. Includes both automated methods and human-cognitive assessments.

Program Management

Business and Process Analysis: The discipline of identifying opportunities to improve or optimize business processes and determining solutions to business problems. Automating analyzed processes often leads to system development.

Portfolio Management: The practice of coordinating multiple projects including resource and schedule planning, and prioritization. It also describes the administration of a collection of applications or of services.

Program Management: The collection of actions required to manage a number of related projects having cross-project dependencies to achieve an aggregate result, or end state.

Project Management: The action of marshaling resources, planning and executing a defined project. Its activities include project initiation, planning and coordination, monitoring and control, and reporting and communication.

Project Budgeting and Reporting: The specific activity of planning resource allocation to a project and monitoring and reporting the consumption of project resources to the project sponsors.

Strategy and Planning

Enterprise Architecture: The discipline of defining the information structure of the organization including its components (information assets, computer systems, and applications) and their relationships. EA describes present and future states of the organization.

IT Purchasing: The collection of activities required to strategically source materials, supplies and other resources necessary to the delivery of IT services.

IT Service Continuity Planning: The planning and preparations for mitigating disaster events and the analysis of supported business processes required to prioritize recovery operations. (DR)

Annual and Long Range Planning: The practices of making yearly plans, and multi-year (biennium and beyond) plans for technology service delivery.

Operating and Capital Budgeting and Reporting: The development, monitoring, and periodic reporting of:

An operating budget which classifies functions by accounting codes and tracks maintenance, repairs, salaries and contracts; and

A capital budget for new equipment, replacement equipment, research and development, and other investment expenditures.

Vendor and Contract Management: The development and maintenance of vendor relationships and monitoring of contract performance and value.

Dimension 3: Processes

By definition, a process is a set of structured activities to achieve an objective. A process entails several components: objective, trigger, supplier(s) to the process, input(s), transformational activities, outputs, customers of the process, roles, and measurements. Definition of these elements clarifies how work should be done across organizational boundaries, while also aligning boundaries and interfaces between processes. These elements are defined in a variety of documents such as policies, process definition documents, standards, work instructions, etc. Together, these documents and their content provide tools and management controls to ensure that work results conform with objectives and other requirements.

Process Reference Model

The process Reference Model below outlines key and essential IT service management and project management processes that will be standardized across all agencies. These are primarily cross-functional processes. The model below is organized around the five phases of the service life-cycle as defined by ITIL, with a sixth column for project management. Definitions for these processes are contained in Appendix A.

Common Agency Processes for Managing IT Services

Service Strategy	Service Design	Service Transition	Service Operation	Continual Service Improvement	Project & Portfolio Management
Strategy Management for IT Services Service Portfolio Management Financial Management for IT Services Demand Management Business Relationship Management	Design Coordination Service Catalogue Management Service Level Management Availability Management Capacity Management IT Service Continuity Management Information Security Management Supplier Management	Transition Planning & Support **Change Management** Service Asset and Configuration Management Release and Deployment Management Service Validation and Testing Change Evaluation Knowledge Management	**Event Management** **Incident Management** **Request Fulfillment** Problem Management Access Management	Seven-step Improvement	**Project Management** Project Portfolio Management

Within this process model, the following processes have been selected for early development integration, while those remaining will be sequenced based on a process maturity assessment. Sample process documentation will be reviewed by a cross-agency team and shared under separate cover.

Incident Management – restores normal service operation as quickly as possible and minimizes the adverse impact on the customer operations, thus ensuring that agreed levels of service quality are maintained.

Request Fulfillment – provides a channel for users to request and receive standard services for which a predefined authorization and qualification process exists; manages the lifecycle of all service requests from users.

Change Management – control the lifecycle of all changes, enabling beneficial changes with minimum disruption to IT services. Ensures changes are recorded and evaluated, and that authorized changes are prioritized, planned, tested, implemented, documented and reviewed in a controlled manner.

Event Management – monitoring of systems in order to detect, make sense of and manage events throughout their lifecycle.

Project Management - Project Management processes apply knowledge, skills, tools and techniques to initiate, plan, execute, monitor/control, and close project activities to meet project requirements.

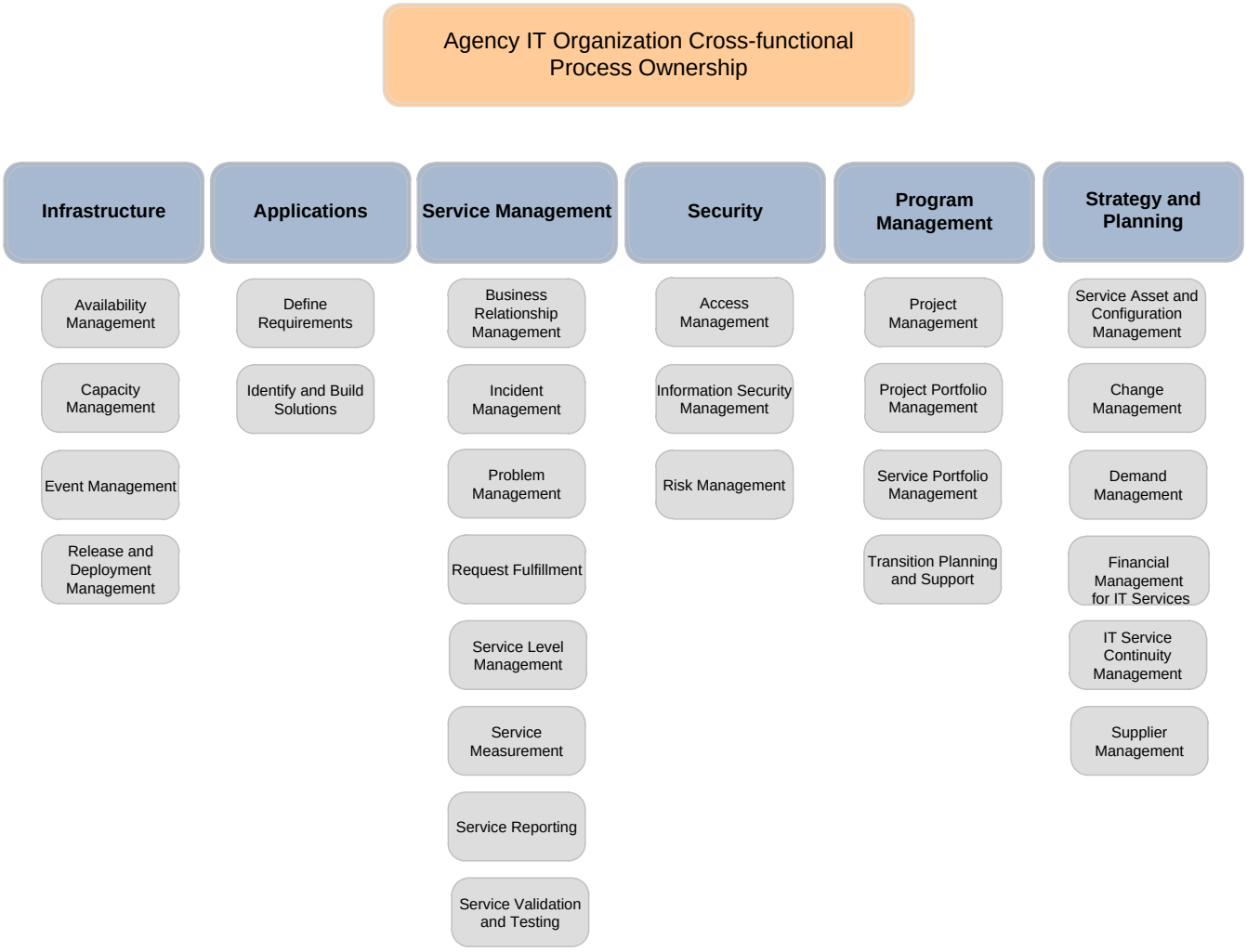
> **Initiation** – The activities within this process group define a new project by obtaining authorization to start the project. The initial scope is defined and initial financial resources are committed. Internal and external stakeholders are identified and a project manager is assigned.
>
> **Planning** – The activities within this process group define the total scope of the effort, refine the objectives, and develop the course of action to achieve the objectives
>
> **Executing** – The activities within this process group involve carrying out the work defined during the planning process. This work includes coordinating people and resources, acquiring and managing the project team, procurement, and managing stakeholder expectations.
>
> **Monitoring / Controlling** – The activities within this process group are required to track, review and monitor project progress and performance, and manage changes to the project.
>
> **Closing** – The activities within this process group are performed to formally complete the project. This work includes: obtaining acceptance by the customer or sponsor, project close review and lessons learned, archiving all relevant project documents, and closing out procurement.

Note: The project management descriptions above are adapted from the PMBOK Guide, Fourth Edition.

Process Ownership

Although the above processes require multiple functions to contribute inputs to the ultimate outcome, each process must have a single, clearly defined functional "owner" – the group that is responsible for the management and the outcomes of the process.

The following illustration identifies which common agency functions will own each process. The manager of the function serves as the process owner for the designated processes. A process owner champions the process, ensures it is adequately resourced, designs the process and its elements, continually improves the process and ensures objectives are met.


Agency IT Organization Cross-functional Process Ownership
Infrastructure
Availability Management
Capacity Management
Event Management
Release and Deployment Management
Applications
Define Requirements
Identify and Build Solutions
Service Management
Business Relationship Management
Incident Management
Problem Management
Request Fulfillment
Service Level Management
Service Measurement
Service Reporting
Service Validation and Testing
Security
Access Management
Information Security Management
Risk Management
Program Management
Project Management
Project Portfolio Management
Service Portfolio Management
Transition Planning and Support
Strategy and Planning
Service Asset and Configuration Management
Change Management
Demand Management
Financial Management for IT Services
IT Service Continuity Management
Supplier Management

Dimension 4: Common Enabling Tools

All agencies will utilize appropriate tools to implement and manage the priority processes listed above:

- Incident management
- Request fulfillment
- Project management
- Change management
- Event management

As a first step, agencies will document the current tools that they use in order to identify the opportunity for shared tools at the enterprise level.

Appendix 1: Process Definitions

Service Strategy Processes

Service Strategy processes define the strategies, policies, resources, constraints and objectives for delivering IT services.

Strategy Management for IT Services – articulate how IT will enable its customers to achieve their business outcomes; develop strategies, objectives and policies; assess constraints and allocate resources.

Service Portfolio Management – ensure the right mix of services to balance the investment in IT with the ability to meet business outcomes. Tracks the investment in services throughout their lifecycle and works with other service management processes to ensure that the appropriate returns are being achieved. Also ensures that services are clearly defined and linked to the achievement of business outcomes, thus ensuring that all design, transition and operation activities are aligned to the value of the services.

Financial Management for IT Services – manages budgeting, accounting and charging requirement. Also quantifies the value that State IT services contribute to the Executive Branch.

Demand Management – understand, anticipate and influence customer demand for services and to work with capacity management to ensure the service provider has capacity to meet this demand. Also works at every stage of the lifecycle to ensure that services are designed, tested and delivered at the right level of activity to support business outcomes.

Business Relationship Management – provide links between State IT and customers at the strategic and tactical levels. The purpose of these links is to ensure that State IT understands the business requirements of customers and is able to provide services that meet these needs.

Service Design Processes

Service Design processes design IT services, processes and policies to build, test and deploy IT services.

Design Coordination – ensure the goals and objectives of the Service Design phase are met by providing and maintaining a single point of coordination and control for all activities and processes within Service Design.

Service Catalog Management – provides and maintains a single source of consistent information on all operational services and those being prepared to be run operationally, and to ensure that it is widely available to those who are authorized to access it.

Service Level Management – agrees and documents service level targets and responsibilities within SLAs and service level requirements for every service and related activity within IT. Ensure that all current and planned IT services are delivered to agreed achievable targets.

Availability Management – ensured the level of availability for IT Services and supporting components meets the agreed service levels in a cost-effective and timely manner.

Capacity Management – ensure the capacity of IT services meet the agreed capacity and performance-related requirements in a cost-effective and timely manner; does this for current and future capacity and performance needs.

IT Service Continuity Management – supports the Executive Branch's overall business continuity process by ensuring that, by managing the risks that could seriously affect IT services, that State IT can always provide minimum agreed business continuity-related service levels.

Information Security Management – aligns IT security with business security of the Executive Branch and ensures that the confidentiality, integrity and availability of assets, information, data and IT services always match the agreed needs of the Executive Branch.

Supplier Management – ensures that suppliers and the services they provide are managed to support IT service targets and business expectations.

Service Transition Processes

Service Transition processes makes sure the new, modified, and retired services meet the requirements of the business as IT services are transitioned (built, tested, deployed) into or out of operations.

Transition Planning & Support – provide overall planning for service transitions and coordinate the required resources.

Change Management – control the lifecycle of all changes, enabling beneficial changes with minimum disruption to IT services. Ensures changes are recorded and evaluated, and that authorized changes are prioritized, planned, tested, implemented, documented and reviewed in a controlled manner.

Service Asset & Configuration Management – ensure assets required to deliver a service are properly controlled and that accurate, reliable information about these assets is available when and where needed.

Release and Deployment Management – plan, schedule and control the build, test and deployment of releases (bundles of related service or infrastructure changes) and deliver new functionality required by agencies while protecting the integrity of existing services.

Service Validation and Testing – ensure that a new or changed IT service matches its design specifications and will meet the needs of customers.

Change Evaluation – assess the actual performance of an approved change against its intended and predicted performance.

Knowledge Management – provide the best available knowledge, information and data to the right person at the right time to enable improved decision-making.

Service Operation Processes

Service Operation processes coordinates and carries out the activities necessary to deliver IT services to customers at the agreed service levels.

Event Management - detect, make sense of and manage events throughout their lifecycle.

Incident Management – restores normal service operation as quickly as possible and minimizes the adverse impact on the customer operations, thus ensuring that agreed levels of service quality are maintained.

Request Fulfillment – provides a channel for users to request and receive standard services for which a predefined authorization and qualification process exists; manages the lifecycle of all service requests from users.

Problem Management – minimize the customer-impact of incident and problems based on errors in the IT infrastructure; proactively prevent recurrence incidents related to these errors.

Access Management – provides rights for users to access a service or group of services based on the policies and actions defined by information security management.

Continual Service Improvement

Continual Service Improvement has a single process.

Seven-step Improvement – define and manage improvements to IT services and service management processes.

Project Management Processes

Project Management processes apply knowledge, skills, tools and techniques to initiate, plan, execute, monitor/control, and close project activities to meet project requirements.

Initiation – The activities within this process group define a new project by obtaining authorization to start the project. The initial scope is defined and initial financial resources are committed. Internal and external stakeholders are identified and a project manager is assigned.

Planning – The activities within this process group define the total scope of the effort, refine the objectives, and develop the course of action to achieve the objectives

Executing – The activities within this process group involve carrying out the work defined during the planning process. This work includes coordinating people and resources, acquiring and managing the project team, procurement, and managing stakeholder expectations.

Monitoring / Controlling – The activities within this process group are required to track, review and monitor project progress and performance, and manage changes to the project.

Closing – The activities within this process group are performed to formally complete the project. This work includes: obtaining acceptance by the customer or sponsor, project close review and lessons learned, archiving all relevant project documents, and closing out procurement.

Note: The descriptions above are adapted from the PMBOK Guide, Fourth Edition.

Project Portfolio Management

Project Portfolio Management process provide an approach to achieving strategic goals by selecting, prioritizing, assessing, and managing projects, programs and other related work based upon their alignment and contribution to the organization's strategies and objectives.

Selection – This process produces a short list of projects based on the organization's selective criteria. The outcome is a list of projects and/or programs that are ready for prioritization.

Prioritization – This process *ranks* the projects and / or programs according to established criteria. The outcome is a prioritized list of projects and / or programs with the greatest potential to collectively support the organization's strategic initiatives and objectives.

Portfolio balancing – This process *develops* the mix of projects and programs that have the greatest potential, to collectively support the organization's strategic initiatives and objectives.

Authorization – This process formally allocates financial and human resources to either develop business cases or execute selected projects and / or programs.

Portfolio Reporting and Review – This process gathers performance indicators, provides reporting on them, and reviews the portfolio at an appropriate predetermined frequency, to ensure both alignment with the organizational strategy and effective resource utilization.